Grid Security

R= T x C x V

Arkansas Legislature

Joint Energy Committee

3.16

R= T x C x V

- Risk is the product of Threat, Consequence and Vulnerability
  - Well accepted security methodology-
- Threat- where does the danger or harm come from
  - Who are the adversaries?
  - What are their capabilities?

R= T x C x V

- What are the potential targets?

- Consequence- ramifications of a successful attack
  - Safety
  - Reliability
  - Financial
  - Compliance
  - Reputation

R= T x C x V

- Vulnerability- likelihood of a successful attack
  - Defense in depth for Key Targets
  - Strategies designed to:
    - Deter
    - Detect
    - Delay
    - Respond
- We do not have control over the Threat
- We can however control Consequence
  - Design resiliency into the system
  - Obtain spare parts in order to make quicker repairs
- We can also influence Vulnerability
  - Security measures
  - Policies and procedures designed to increase security

Just like in the Martial Arts:
The Key is to Find the Balance

Design Basis Threat

- The NERC Physical Security Advisory Group recently created a Design Basis Threat document to help the industry better understand the threat
- PSAG is made up of 25 subject matter experts from NERC, industry, and government
- The DBT is a living document that will be regularly updated to include new threat actors and threat vectors

Our Approach

- Leverage NERC CIP standards including CIP 014 to establish the foundation for physical and cyber security for critical assets
- Implement best practice techniques that go above and beyond the regulatory requirements where feasible
- Establish a tiered approach to substation criticality
- Create a menu of security measures for each tier
- Leverage outages and construction projects to install the appropriate security measures for the tier
- Partner with 7 other electric utilities and energy companies to establish Grid Assurance